REMARKS

The Examiner has rejected Claims 1-5, 7, 12-16, 18, 23, 26, 29, and 33 under 35 U.S.C. 103(a) as being unpatentable over ConSeal PC FIREWALL Technical Summary (hereinafter ConSeal) in view of Hari et al. (Detecting and resolving packet filter conflicts) in view of Coss et al. (U.S. Patent No. 6,098,172). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to the independent claims. Specifically, applicant has amended the independent claims to at least substantially include the subject matter of former dependent Claim 10 et al.

With respect to the independent claims, the Examiner has relied pages 1-2 from the ConSeal reference below to make a prior art showing of applicant's claimed "...executing security actions associated with the active policies if associated limits are met" (see this or similar, but not necessarily identical language in the independent claims).

"ConSeal PC FIREWALL Technical Information

* Runs on any Windows 95/98 or Windows NT 3.51 and 4.0 platform with a serial or Ethernet device
* Filters all data packets by capturing them at the device (link layer) level, including IP (e.g. TCP, UDP, ICMP), NetBEUI, IPX, ARP, etc.
* Filters all services - file and printer shares, protocols that use Winsock (e.g. SMTP, HTTP) and operating system services (e.g. ping, rip, FTP, Telnet)
* Application and service transparency (i.e. no plug-ins or add-ons to enable applications or services to pass through the firewall)
* Controls access to system resources, including IP address specific filtering
* Manual, automatic, checked and unchecked learning modes
* Constant monitoring for all traffic passing in or out of the system
* Environment sensitive rulesets-rulesets for when a specific application runs, for a specific driver, for a dialup phone number X, for a VPN device, etc. The system manages rulesets activation and conflicts behind the scenes.
* User-friendly ruleset viewing, editing and display tools
* Optional password protection of rulesets
* Compatibility with all other Windows 95/98 and Windows NT 3.51 and 4.0 encryption and security software
* Year 2000 compliant

> * Complete logging services" (ConSeal, Page 1 - emphasis added)

Applicant respectfully asserts that the excerpt(s) from ConSeal as relied upon by the Examiner teaches that the "...system manages rulesets activation and conflicts behind the scenes" (emphasis added). However, the ConSeal excerpt fails to disclose a technique of "...executing security actions associated with the active policies if associated limits are met" (emphasis added), as claimed by applicant.

In the Office Action mailed 05/05/2006, the Examiner argued that "each time a packet is filtered (i.e. not allowed through the firewall) that is the ConSeal firewall executing a security action associated with the active policies when a limit is met." However, applicant respectfully asserts that ConSeal discloses "[f]ilter[ing] all data packets by capturing them at the device (link layer) level, including IP (e.g. TCP, UDP, ICMP), NetBEUI, IPX, ARP, etc" and "[f]ilter[ing] all services - file and printer shares, protocols that use Winsock (e.g. SMTP, HTTP) and operating system services (e.g. ping, rip, FTP, Telnet)" (emphasis added). Clearly, the disclosure in ConSeal of filtering all data packets and all services fails to even suggest "...executing security actions associated with the active policies if associated **limits** are met" (emphasis added), in the manner as claimed by applicant.

In addition, the Examiner has relied on the page 1204, section II from the Hari reference below to make a prior art showing of applicant's claimed technique "...wherein a first policy with a higher priority has a first condition associated therewith that is different from a second condition associated with a second policy with a lower priority such that the first policy and second policy are activated under different priority-related conditions" and "... identifying currently executed security actions, determining whether a conflict exists between the currently executed security actions, and resolving any conflicts between the currently executed security actions" (see this or similar, but not necessarily identical language in the independent claims).

> "a) The first matching filter in the filter database takes precedence. For example, if F1 is stored before F2 in the

> database, then the flow goes through at 100 Mbps. On the other hand, if F2 is stored before F1, than most packets of the flow are dropped, since the flow is restricted to a BW of only 1 Mbps. This approach is commonly used to resolve conflicts in firewalls, where incoming packets are matched against filters specified in access control lists and the action is determined by the first matching filter.
> b) **Assign priorities to difference filters, and use the matching filter with the highest priority.** This scheme turns out to be identical to scheme a) if we sort the fitlers in the order of priority.
> c) **Assign priorities to fields so that in case of multiple matches the filter with the most specific matching field with the highest priority is selected.** For example, if the source address is given higher priority on matches than the destination address, then for packets going from network X to network Y the filter F1 is a better match than F2." (Hari, page 1204, section II - emphasis added)

Applicant respectfully asserts that the excerpt from Hari relied upon by the Examiner teaches a method conflict resolution where one filter is selected over other potential filters. Specifically, for conflict resolution, the Hari excerpt referenced above teaches three conflict resolution techniques. The first conflict resolution technique disclosed teaches that "[t]he first matching filter in the filter database takes precedence" (emphasis added). The second conflict resolution technique disclosed teaches to "[a]ssign priorities to difference filters, and use the matching filter with the highest priority" (emphasis added). The third conflict resolution technique disclosed teaches to "[a]ssign priorities to fields so that in case of multiple matches the filter with the most specific matching field with the highest priority is selected" (emphasis added).

Thus, excerpt from Hari referenced above actually *teaches away* from applicant's claimed technique "...wherein a first policy with a higher priority has a first condition associated therewith that is different from a second condition associated with a second policy with a lower priority such that the first policy and second policy are activated under different priority-related conditions" (emphasis added), as claimed by applicant, since Hari teaches that a selection of the filters is based on the same priority-related condition [namely, condition a), b), or c) in the above excerpt]. Note that Hari does not teach that a first filter is selected based on technique a) while a second filter is selected based on technique b), etc.

In the Office Action mailed 05/05/2006, the Examiner argued that "the priority based system of Hari teaches that each filter (i.e. policy) has a different priority and when a packet matches more than one filter, which ever filter has a higher priority is used." Again, applicant respectfully asserts that Hari teaches, during conflict resolution, either selecting the first matching filter, the matching filter with the highest priority, or the filter with the most specific matching field with the highest priority. Again, applicant respectfully disagrees with the Examiner's rejection, since Hari teaches that a selection of the filters is based on the same priority-related condition [namely, condition a), b), or c) in the above excerpt]. Again, only applicant teaches and claims a technique "wherein ... the first policy and second policy are activated **under different priority-related conditions**" (emphasis added), as claimed by applicant.

Also, with respect to independent Claim 28, the Examiner has rejected the same under 35 U.S.C. 103(a) as being unpatentable over ConSeal, in view of Hari, in view of Brock et al. (U.S. Patent No. 2003/0110393). Specifically, the Examiner has relied upon the following excerpt from Brock to make a prior art showing of applicant's claimed technique "wherein the conditions represent an urgency associated with an issue causing the policy to be activated" (emphasis added).

> "[0005] When the intrusion detection system observes activity that is suggestive or indicative of an intrusion, for example when the value of a signature event counter crosses its associated signature threshold, the IDS may generate an alert. **The purpose of the alert is to inform a network administrator of the intrusion, so that the administrator may act to minimize the damage done by the intruder. The alert may include other information drawn from the particular signature that is associated with the suspected intrusion, such as a priority or importance level suggesting the urgency of the need for defensive action,** or instructions or data to help the administrator limit the damage done by the intruder." (Brock, Paragraph 0005 - emphasis added)

Applicant respectfully asserts that the excerpt relied upon by the Examiner teaches that the "alert is to inform a network administrator of the intrusion, so that the administrator may act to minimize the damage done by the intruder" (emphasis added).

Further, the "alert may include ... a priority or importance level suggesting the urgency of the need for defensive action." However, an administrator action to an alert fails to disclose a technique "wherein the conditions represent an urgency associated with an issue causing the policy to be activated" (emphasis added), as claimed by applicant.

In the Office Action mailed 05/05/2006, the Examiner argued that "Brock teaches including an indication of urgency with an alert when a condition is met and since the indication is based on conditions being met causing the administrator to act the are causing a policy to be activated." Clearly, Brock's disclosure that "the administrator may act to minimize the damage done by the intruder" (emphasis added) fails to even suggest a technique "wherein the conditions represent an urgency associated with an issue causing the policy to be activated" (emphasis added), as claimed by applicant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has incorporated the subject matter of former Claim 10 et al. into the independent claims.

With respect to the subject matter of former Claim 10 et al. (now at least substantially incorporated into the independent claims), the Examiner has rejected the same under 35 U.S.C. 103(a) as being unpatentable over ConSeal, in view of Hari, in view of Coss, and in further view of Beebe et al. (U.S. Publication No. 2001/00141150). Specifically, the Examiner relied upon the following excerpt from Beebe to make a prior art showing of applicant's claimed technique "wherein the conditions include a source of the policies."

> '[0227] Referring to FIG. 12E, in step 902, corporate-dictated rules, similar to those described previously with reference to FIGS. 12C and 12D, that will comprise the basic security policy to be distributed downward from the "corporate" level 806 to each "regional" level 808 Firewall Management Server 26 (such as the one in San Francisco 814), and to each "branch" level 810 Firewall Management Server 26 (such as those in Salt Lake City 820 and Denver 822), are defined. In step 904 the corporate-dictated rules are merged into the current Security Rule Base 102 of the Security Policy 100. As mentioned previously, the corporate-dictated rules will have priority over and remove any conflicting rules. In step 906, the updated Security Policy 100 is downloaded to the local Line Sensors 18 on the "corporate" level 806.' (Beebe, Paragraph 0227 - emphasis added)

Applicant respectfully asserts that the excerpt from Beebe relied upon by the Examiner teaches that 'the basic security policy [is] to be distributed downward from the "corporate" level ... to each "regional" level ... and to each "branch" level' (emphasis added). During the downward distribution, the "corporate-dictated rules will have priority over and remove any conflicting rules" (emphasis added). The excerpt from Beebe thus merely teaches rules for "basic security policy" distribution and fails to make any disclosure where "...conditions include a source of the policies" (emphasis added), as claimed by applicant.

In the Office Action mailed 05/05/2006, the Examiner argued that "the rules of Beebe are based on the source of the rules and every rule has conditions; therefore Beebe teaches the conditions include a source of the policy." Applicant respectfully disagrees. Specifically, with respect to Beebe's teaching, applicant respectfully asserts that Beebe merely discloses that "corporate-dictated rules will have priority over and remove any

conflicting rules" (emphasis added). Thus, the fact that corporate-dictated rules simply remove any conflicting rules in Beebe fails to disclose (and even *teaches away* from) applicant's claimed technique for activating policies whose associated conditions are determined to be met, "wherein the conditions include a source of the policies" (as claimed by applicant- emphasis added).

Again, applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. With respect to Claims 2 and 3 et al., the Examiner has relied on the following excerpt from ConSeal to make a prior art showing of applicant's claimed technique "...comprising determining whether a user confirms the activation of the policies" (see this or similar, but not necessarily identical language in former dependent Claims 2 and 13) and "...comprising activating the policies if the user confirms" (see this or similar, but not necessarily identical language in former dependent Claims 3 and 14).

> "ConSeal PC FIREWALL's learning modes allow rules and rulesets to be generated efficiently and straightforwardly. The Manual Learning Mode allows users to add, edit and delete their rules and tweak them according to address, service type and so on. The **Checked Learning Mode prompts the user for rule generation when it encounters a packet for which it has no rule.** The Unchecked Learning Mode allows users to generate rules in the background by performing their normal networking activities over a trial period." (ConSeal, Page 2 - emphasis added)

Applicant respectfully asserts that the excerpt from ConSeal relied upon by the Examiner merely teaches a technique where the "Checked Learning Mode prompts the user for rule generation when it encounters a packet for which it has no rule" (emphasis added). However, there is no disclosure of "determining whether a user confirms the activation of the policies" (emphasis added) and "activating the policies if the user

confirms" (emphasis added), as claimed by applicant. Thus, the ConSeal excerpt fails to disclose all of applicant's claimed technique.

In the Office Action mailed 05/05/2006, the Examiner argued that "when a rule in ConSeal has not been used before and the system is in Checked Learning Mode, the user is prompted to make a rule for the packet (i.e. allow or disallow)" and "[w]hen the user selects an action the user is confirming the activation of the rule." Applicant respectfully asserts that ConSeal discloses that "Checked Learning Mode prompts the user for rule generation when it encounters a packet for which it has no rule" (emphasis added). Clearly, prompting a user for rule generation when no rule exists fails to even suggest "determining whether a user confirms the activation of the policies" (emphasis added) and "activating the policies if the user confirms" (emphasis added), as claimed by applicant. Applicant asserts that ConSeal's prompt for "rule generation" simply fails to even suggest any "activation of the policies," as claimed by applicant.

Further, with respect to Claims 4-5 and 15-16, the Examiner has relied on the following excerpts from Page 2 of ConSeal to make a prior art showing of applicant's claimed "updating the set of policies" (see this or similar, but not necessarily identical language in dependent Claims 4 and 15), "wherein the updating includes receiving another inactive policy, determining whether the user accepts the inactive policy, and adding the inactive policy to the set if the user accepts the inactive policy" (see this or similar, but not necessarily identical language in dependent Claims 5 and 16).

> "* Protect access to rulesets. For example, do not allow anyone without the password to change rulesets. This would allow a system administrator to force a rule that would disallow print shares over a VPN connection.
> * Experts and novices can develop rulesets easily or allow them to be generated by system usage." (ConSeal, Page 2 - emphasis added)
>
> "* ConSeal PC FIREWALL's learning modes allow rules and rulesets to be generated efficiently and straightforwardly. The Manual Learning Mode allows users to add, edit and delete their rules and tweak them according to address, service type and so on. The Checked Learning Mode prompts the user for rule generation when it encounters a packet for which it has no rule. The Unchecked Learning Mode allows users to generate rules in the background by

performing their normal networking activities over a trial period." (ConSeal, Page 2 - emphasis added)

Applicant respectfully asserts that the above excerpts from ConSeal as relied upon by the Examiner disclose a technique to "[p]rotect access to rulesets... [to] ...allow a system administrator to force a rule" and that "[e]xperts and novices can develop rulesets" (emphasis added). However, the ConSeal excerpts fail to even suggest a technique "wherein the updating includes receiving another inactive policy, determining whether the user accepts the inactive policy, and adding the inactive policy to the set if the user accepts the inactive policy" (emphasis added), as claimed by applicant. There is simply no disclosure on "receiving another inactive policy" (emphasis added), as claimed by applicant.

In the Office Action mailed 05/05/2006, the Examiner argued that "ConSeal allows for an administrator to make a rule remotely and a user can download this rule (as evidenced by page 4 of the Mien reference supplied on 09/21/2005)." Further, the Examiner argued that "[w]hen a user chooses to download a policy it is inactive and by going to download the policy the user is inherently accepting it." Applicant respectfully asserts that the excerpt from Mien discloses that "you might want to download the cable modem rules set from the support section of the Signal9 website." In addition, Mien discloses to "[s]imply uncompress [rules_cable.zip] into your CFW directory, and do a File, Change Rules set File from the main menu to load it in, and you're done." However, disclosing that the user may download rules, uncompress the rules, and load the rules in, fails to suggest "determining whether the user accepts the inactive policy..." (emphasis added), as claimed by applicant. In addition, downloading a set of rules fails to disclose receiving an "inactive policy" which is not added until "the user accepts the inactive policy," as claimed by applicant.

In addition, with respect to Claims 11 and 22, the Examiner has rejected the same under 35 U.S.C. 103(a) as being unpatentable over ConSeal, in view of Hari, in view of Coss, and in further view of Porras et al. (U.S. Patent No. 6,704,874). Specifically, the Examiner has relied upon the following excerpt from Porras to make a prior art showing

of applicant's claimed technique "wherein the conditions include a severity of security actions associated with the policies" (see this or similar, but not necessarily identical language in dependent Claims 11 and 22).

> "In a further aspect, alerts may be tagged with a priority indication flag formulated against the remote processing station's alert processing policy and tagged with a relevance flag that indicates the likely severity of the attack with respect to the known internal topology of the monitored network." (Porras, Col. 2, lines 46-51 - emphasis added)

Applicant respectfully asserts that the above excerpt from Porras merely teaches a technique where "alerts may be tagged with a priority indication flag ... and tagged with a relevance flag that indicates the likely severity of the attack" (emphasis added). Tagging alerts in no way even suggests a technique "wherein the conditions include a severity of security actions associated with the policies" (emphasis added), as claimed by applicant.

In the Office Action mailed 05/05/2006, the Examiner argued that "Porras teaches tagging alerts with a flag indicating the severity of the attack" and that "[t]hese alerts are generated based on filtering conditions being met (see column 1 lines 51-62) and therefore are associated with the conditions being met." Applicant respectfully asserts that Porras discloses that "[f]iltering may also include tagging alerts with a significance score that can indicate a priority measure and relevance measure" (emphasis added). However, merely tagging alerts to indicate a priority measure fails to suggest a technique "wherein the conditions include a severity of security actions associated with the policies" (emphasis added), as claimed by applicant.

Again, applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

To this end, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P048/01.183.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100